

DarkComet RAT Malware Hidden Inside Fake Bitcoin Tool

 pointwild.com/threat-intelligence/darkcomet-rat-malware-hidden-inside-fake-bitcoin-tool

Lat61 Threat Intelligence Team

November 11, 2025

DarkComet RAT Malware Hidden Inside Fake Bitcoin Tool Malware Analysis Report

Introduction

The rise of cryptocurrency has not only transformed global finance but has also opened new opportunities for cybercriminals. Bitcoin, being the most recognized digital currency, has become a common lure in social engineering campaigns. Attackers frequently disguise their malware as Bitcoin wallets, mining software, or trading tools to trick unsuspecting users into executing them.

One such case is the reappearance of DarkComet RAT, a well-known remote access trojan that, despite being discontinued by its creator years ago, continues to circulate in underground forums and attack campaigns. DarkComet is notorious for its rich set of spying and control features, ranging from keystroke logging and file theft to webcam surveillance and remote desktop control.

The sample analyzed in this post masquerades as a Bitcoin-related application, appealing to individuals interested in cryptocurrency. Once installed, instead of delivering the promised functionality, it silently activates the full arsenal of “DarkComet RAT”. This highlights two key aspects of the modern threat landscape:

1. **Old malware never truly dies:** Once publicly leaked, families like DarkComet are repurposed indefinitely.
2. **Cryptocurrency remains a prime attack vector:** Lures involving Bitcoin or digital assets continue to be highly effective against both casual users and investors.

This blog takes a closer look at the technical behavior of this Bitcoin themed DarkComet variant, examining how it operates, what capabilities it delivers to the attacker, and why cryptocurrency enthusiasts should remain cautious when downloading wallet tools or trading utilities from unverified sources.

Initial Discovery

The malware sample was obtained in the form of a compressed RAR archive, a common tactic used by threat actors to evade detection and lower suspicion. By packaging malicious executables inside archive files, attackers aim to:

- **Bypass email and web filters** that may block direct executable attachments.
- **Reduce antivirus detection rates**, since the archive format can conceal malicious payloads until extraction.
- **Encourage user interaction**, as the victim must manually extract and run the file, which attackers often disguise as a legitimate tool.

Upon inspection, the RAR file contained a single executable masquerading as a **Bitcoin wallet or utility application**. The naming convention and iconography suggested that the attacker was targeting cryptocurrency enthusiasts, leveraging Bitcoin as the lure.

Key observations during triage included:

- **Archive Type:** RAR compressed file
- **Contained Payload:** Executable disguised as Bitcoin software
- **Likely Delivery Method:** Could have been distributed via phishing emails, malicious forums, or file-sharing platforms
- **Attacker Goal:** To trick users into extracting and launching the RAT under the belief that they were opening a cryptocurrency related program

The use of a RAR archive adds an additional layer of deception, as many users consider compressed files harmless and are more likely to extract them without thorough inspection. This approach aligns with common **malware delivery patterns**, where attackers combine social engineering (in this case, cryptocurrency interest) with technical evasion (RAR compression) to maximize infection success rates.

File Info of Compressed file

MD5: dbedd5e7481b84fc5fa82d21aa20106f

SHA-1: 87a2425098d257f4c0450a0cf56d0209963096d4

SHA256: 11bf1088d66bc3a63d16cc9334a05f214a25a47f39713400279e0823c97eb377

File Size: 255.23 KB

File Type: RAR

Upon decompression it decompresses to “94k BTC wallet.exe” which is UPX Packed

File Info of Decompressed file

| 94k BTC wallet.exe | |
|--------------------|---|
| Property | Value |
| File Name | D:\New\PointWild\upx-4.2.2-win64\94k BTC wallet.exe |
| File Type | Portable Executable 32 |
| File Info | UPX v0.89.6 - v1.02 / v1.05 -v1.22 (Delphi) stub |
| File Size | 318.00 KB (325632 bytes) |
| PE Size | 318.00 KB (325632 bytes) |
| Created | Wednesday 29 October 2025, 14.16.48 |
| Modified | Monday 21 December 2020, 14.49.54 |
| Accessed | Thursday 30 October 2025, 12.41.33 |
| MD5 | 46BCF4E361CD251C958720E1198E3F0A |
| SHA-1 | 57AB0765C97B230C615B43EE4EBC28B674887121 |

Figure 1: File Info image

File Name : 94k BTC wallet.exe

MD5 : 46bcf4e361cd251c958720e1198e3f0a

SHA-1 : 57ab0765c97b230c615b43ee4ebc28b674887121

SHA256 : 5b5c276ea74e1086e4835221da50865f872fe20cfc5ea9aa6a909a0b0b9a0554

File Size : 318.00 KB

File Type : Win32 EXE (Portable Executable 32)

PEiD packer : UPX v0.89.6 – v1.02 / v1.05 -v1.22 (Delphi) stub

Technical Analysis:

Unpacking a Suspicious Bitcoin Wallet Executable

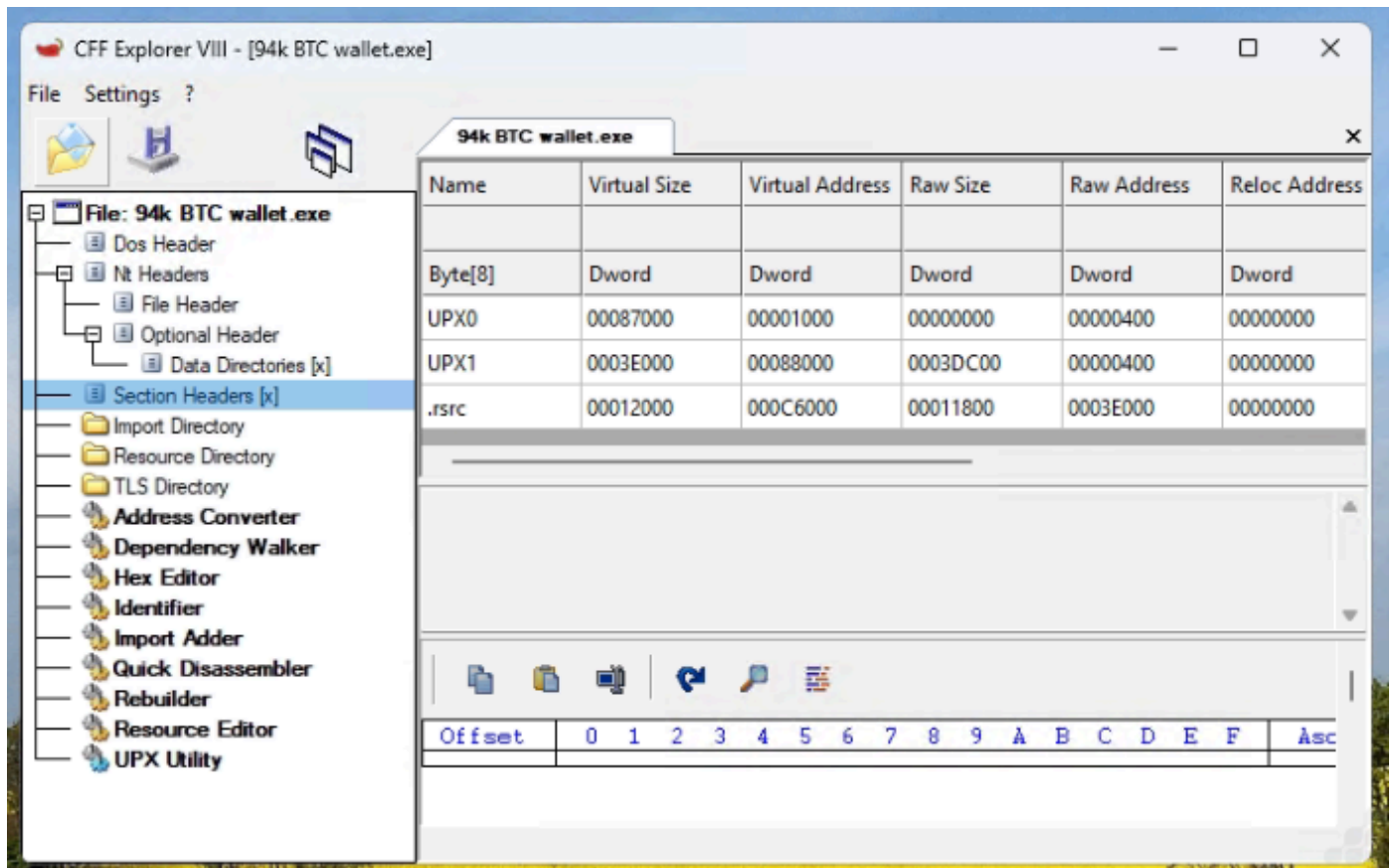


Figure 2: UPX Packed

During static analysis of the suspicious executable “94k BTC wallet.exe”, the first step was to check the PE (Portable Executable) structure using CFF Explorer. This revealed that the sample was packed with UPX (Ultimate Packer for Executables) a common method malware authors use to compress and obfuscate executables to evade detection.

Step 1 : Inspecting the Executable in CFF Explorer

When loading the file into CFF Explorer, the Section Headers tab showed the following key details:

Sections present:

- UPX0
- UPX1
- .rsrc

These are strong indicators that the file is packed with UPX. Typically, a clean Windows PE executable contains sections such as .text, .data, .rdata, and .rsrc. The presence of only UPX0 and UPX1 (instead of .text, .data, etc.) means that the code and data have been compressed into UPX containers.

Virtual & Raw Sizes:

The table shows that the UPX0 section has a large virtual size (00087000) but a very small raw size (00000000). This is a red flag: it indicates that the actual code is not directly available on disk but will be unpacked at runtime into memory.

Similarly, the UPX1 section (0003E000 raw size) contains the compressed payload that will be decompressed during execution.

Thus, static inspection confirms the binary is packed and not in its original form.

Step 2 : Unpacking the Executable with [UPX](#) Packer ?

```
Microsoft Windows [Version 10.0.26100.6899]
(c) Microsoft Corporation. All rights reserved.

D:\New\PointWild\upx-4.2.2-win64>upx.exe -d "94k BTC wallet.exe" -o Unpacked94kBTCwallet.exe
      Ultimate Packer for eXecutables
      Copyright (C) 1996 - 2024
UPX 4.2.2      Markus Oberhumer, Laszlo Molnar & John Reiser      Jan 3rd 2024

  File size      Ratio      Format      Name
  -----
  742400 <-      325632      43.86%      win32/pe      Unpacked94kBTCwallet.exe

Unpacked 1 file.

D:\New\PointWild\upx-4.2.2-win64>
```

Figure 3: Successful unpacking of “94k BTC wallet.exe” with UPX 4.2.2

To analyze the actual malicious logic, the executable must be unpacked. The UPX tool provides a built-in decompression option. The following command was used:

```
upx.exe -d “94k BTC wallet.exe” -o Unpacked94kBTCwallet.exe
```

- -d → instructs UPX to decompress the binary.
- -o → specifies the output filename for the unpacked executable.

The unpacking process completed successfully, producing an unpacked file named Unpacked94kBTCwallet.exe.

- Original packed size: 325,632 bytes
- Unpacked size: 742,400 bytes
- Compression ratio: ~43.86%

This confirms that nearly half the original executable had been compressed, and the unpacked binary is now in a state suitable for deeper reverse engineering.

Step 3 : Why Does DarkComet Use UPX Packer ?

DarkComet RAT samples are often packed with UPX (Ultimate Packer for Executables) to make detection and analysis more difficult.

Malware authors behind DarkComet use UPX for the following reasons:

- **Evasion of Static Signatures:**
By compressing and restructuring the executable layout, the DarkComet binary avoids static detections that rely on known byte patterns or file hashes.
- **Obfuscation of Code and Imports:**
Packing hides the real API imports and code structure, which makes it harder for analysts and antivirus engines to understand the malware's behavior through static inspection.
- **Smaller Payload Size:**
The packed executable is smaller in size, helping the attacker distribute it more easily via phishing emails or malicious downloaders.

During analysis, we observed that the DarkComet sample was UPX-packed, and after unpacking, our engine successfully detected and classified the payload as a **Backdoor.DarkComet**.

Although UPX is an open-source packer and easy to reverse with official tools, some DarkComet variants modify UPX headers or add extra encryption layers to slow down the analysis process.

File Info of Unpacked file

| | |
|------------------|--|
| MD5 | : d74ca6016bdde3df525d7c7651747336 |
| SHA-1 | : dc56a542e3db56f1c7132d3e99c960c09396cde3 |
| SHA256 | : 58c284e7bbeacb5e1f91596660d33d0407d138ae0be545f59027f8787da75eda |
| File Size | : 725.00 KB |
| File Type | : Win32 EXE (Portable Executable 32) |
| Compiler | : Borland Delphi (2006) [Professional] |

After unpacking the **UPX packed DarkComet sample (94kBTCwallet.exe)**, we examined the unpacked executable in a PE analysis tool to verify the restoration of original sections.

As shown below, the unpacked binary now displays multiple standard Portable Executable (PE) sections such as **.text**, **.data**, **.rdata**, **.idata**, and others which were previously compressed and hidden inside the UPX-packed version.

| Unpacked94kBTCwallet.exe | | | | | |
|--------------------------|--------------|-----------------|----------|-------------|---------------|
| Name | Virtual Size | Virtual Address | Raw Size | Raw Address | Reloc Address |
| | | | | | |
| Byte[8] | Dword | Dword | Dword | Dword | Dword |
| .text | 0008D8F0 | 00001000 | 0008DA00 | 00000400 | 00000000 |
| .itext | 00001954 | 0008F000 | 00001A00 | 0008DE00 | 00000000 |
| .data | 00003D3C | 00091000 | 00003E00 | 0008F800 | 00000000 |
| .bss | 00007404 | 00095000 | 00000000 | 00093600 | 00000000 |
| .idata | 00004140 | 0009D000 | 00004200 | 00093600 | 00000000 |
| .tls | 00000038 | 000A2000 | 00000000 | 00097800 | 00000000 |
| .rdata | 00000018 | 000A3000 | 00000200 | 00097800 | 00000000 |
| .reloc | 00008ADC | 000A4000 | 00008C00 | 00097A00 | 00000000 |
| .rsrc | 00014C24 | 000AD000 | 00014E00 | 000A0600 | 00000000 |

Figure 4: Unpacked File Details

Persistence Mechanism

In Registry screenshot:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

└─ Path -> C:\Users\admin\AppData\Roaming\MSDCSC\explorer.exe

Figure 5: Registry key

The binary copies itself as explorer.exe under %AppData%\Roaming\MSDCSC\ and creates a Run key for autostart. Ensures execution every system reboot.

Embedded DarkComet Configuration

| | | | | | |
|----------|-------------|-------------|-------------|-------------|-------------------|
| 0236B7A8 | 00 00 00 00 | 50 B2 36 02 | 01 00 00 00 | 97 01 00 00 |P*6..... |
| 0236B7B8 | 23 42 45 47 | 49 4E 20 44 | 41 52 48 43 | 4F 4D 45 54 | #BEGIN DARKCOMET |
| 0236B7C8 | 20 44 41 54 | 41 20 2D 2D | 0D 0A 4D 55 | 54 45 58 3D | DATA --..MUTEX= |
| 0236B7D8 | 78 44 43 5F | 4D 55 54 45 | 58 2D 41 52 | 55 4C 59 59 | {DC_MUTEX-ARULYY |
| 0236B7E8 | 44 7D 0D 0A | 53 49 44 3D | 78 41 50 7D | 0D 0A 46 57 | D}..SID={AP}..FW |
| 0236B7F8 | 42 3D 78 3D | 7D 0D 0A 4E | 45 54 44 41 | 54 41 3D 78 | B={0}..NETDATA={ |
| 0236B808 | 68 76 65 6A | 6F 39 39 31 | 2E 64 64 6E | 73 2E 6E 65 | kvejo991.ddns.ne |
| 0236B818 | 74 3A 31 36 | 30 34 7D 0D | 0A 47 45 4E | 43 4F 44 45 | t:1604}..GENCODE |
| 0236B828 | 3D 78 4D 45 | 68 69 66 64 | 47 35 31 59 | 61 63 7D 0D | = {MEKifdg51Yac}. |
| 0236B838 | 0A 49 4E 53 | 54 41 4C 4C | 3D 78 31 7D | 0D 0A 43 4F | .INSTALL={1}..CO |
| 0236B848 | 4D 42 4F 50 | 41 54 48 3D | 78 33 7D 0D | 0A 45 44 54 | MBOPATH={3}..EDT |
| 0236B858 | 50 41 54 48 | 3D 78 4D 53 | 44 43 53 43 | 5C 65 78 70 | PATH={MSDCSC\exp |
| 0236B868 | 6C 6F 72 65 | 72 2E 65 78 | 65 7D 0D 0A | 48 45 59 4E | lorer.exe}..KEYN |
| 0236B878 | 41 4D 45 3D | 78 65 78 70 | 6C 6F 72 65 | 72 7D 0D 0A | AME={explorer}.. |
| 0236B888 | 45 44 54 44 | 41 54 45 3D | 78 31 36 2F | 30 34 2F 32 | EDTDATE={16/04/2 |
| 0236B898 | 30 30 37 7D | 0D 0A 50 45 | 52 53 49 4E | 53 54 3D 78 | 007}..PERSINST={ |
| 0236B8A8 | 31 7D 0D 0A | 4D 45 4C 54 | 3D 78 31 7D | 0D 0A 43 48 | 1}..MELT={1}..CH |
| 0236B8B8 | 41 4E 47 45 | 44 41 54 45 | 3D 78 30 7D | 0D 0A 44 49 | ANGEDATE={0}..DI |
| 0236B8C8 | 52 41 54 54 | 52 49 42 3D | 78 36 7D 0D | 0A 46 49 4C | RATTRIB={6}..FIL |
| 0236B8D8 | 45 41 54 54 | 52 49 42 3D | 78 36 7D 0D | 0A 53 48 35 | EATTRIB={6}..SH5 |
| 0236B8E8 | 3D 78 31 7D | 0D 0A 53 48 | 36 3D 78 31 | 7D 0D 0A 53 | = {1}..SH6={1}..S |
| 0236B8F8 | 48 37 3D 78 | 31 7D 0D 0A | 53 48 39 3D | 78 31 7D 0D | H7={1}..SH9={1}.. |
| 0236B908 | 0A 43 48 49 | 44 45 46 3D | 78 31 7D 0D | 0A 43 48 49 | .CHIDEF={1}..CHI |
| 0236B918 | 44 45 44 3D | 78 31 7D 0D | 0A 50 45 52 | 53 3D 78 31 | DED={1}..PERS={1 |
| 0236B928 | 7D 0D 0A 4F | 46 46 4C 49 | 4E 45 48 3D | 78 31 7D 0D | }..OFFLINEK={1}. |
| 0236B938 | 0A 23 45 4F | 46 20 44 41 | 52 48 43 4F | 4D 45 54 20 | .#EOF DARKCOMET |
| 0236B948 | 44 41 54 41 | 20 2D 2D 00 | 00 00 00 00 | 00 00 00 00 | DATA --..... |
| 0236B958 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | |
| 0236B968 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | |

Figure 6: Configuration of DarkComet in Memory

This reveals:

- Mutex:DC_Mutex-ARULYYD→ ensures only one instance runs.
- C2 Server: kvejo991.ddns.net over port 1604.
- Install Path: MSDCSC\explorer.exe under user AppData.
- Persistence Flags: Install = 1, Offline keylogging enabled.

This is the hardcoded RAT config extracted post-UPX unpacking

| | | | |
|----------|---------------|-------------------------------|---|
| 0048FA03 | E8 484CF7FF | CALL 94k btc wallet.404650 | |
| 0048FA08 | C3 | RET | |
| 0048FA09 | E9 D653F7FF | JMP 94k btc wallet.404DE4 | |
| 0048FA0E | E8 EE | JMP 94k btc wallet.48F9FE | |
| 0048FA10 | 8D45 B8 | LEA EAX,DWORD PTR SS:[EBP-48] | [ebp-48]: "{88b5ac79-2a3a-11eb-b696-806e6f6e6963-2096026756}" |
| 0048FA13 | E8 0C8DFFFF | CALL 94k btc wallet.488724 | |
| 0048FA18 | 8B55 B8 | MOV EDX,DWORD PTR SS:[EBP-48] | [ebp-48]: "{88b5ac79-2a3a-11eb-b696-806e6f6e6963-2096026756}" |
| 0048FA1B | A1 10494900 | MOV EAX,DWORD PTR DS:[494910] | eax: &"127.0.0.1:1604" |
| 0048FA20 | E8 5F58F7FF | CALL 94k btc wallet.405584 | |
| 0048FA25 | 8D55 B4 | LEA EDX,DWORD PTR SS:[EBP-4C] | [ebp-4C]: "kvejo991.ddns.net:1604" |
| 0048FA28 | B8 A0064900 | MOV EAX,94k btc wallet.4906A0 | eax: &"127.0.0.1:1604", 4906A0: "NETDATA" |
| 0048FA2D | E8 B638FEFF | CALL 94k btc wallet.4735E8 | |
| 0048FA32 | 8B55 B4 | MOV EDX,DWORD PTR SS:[EBP-4C] | [ebp-4C]: "kvejo991.ddns.net:1604" |
| 0048FA35 | B8 E4C34900 | MOV EAX,94k btc wallet.49C3E4 | eax: &"127.0.0.1:1604", 49C3E4: &"kvejo991.ddns.net:1604" |
| 0048FA3A | E8 4558F7FF | CALL 94k btc wallet.405584 | |
| 0048FA3F | A1 E4C34900 | MOV EAX,DWORD PTR DS:[49C3E4] | eax: &"127.0.0.1:1604", 0049C3E4: &"kvejo991.ddns.net:1604" |
| 0048FA44 | 85C0 | TEST EAX,EAX | eax: &"127.0.0.1:1604" |
| 0048FA46 | 74 05 | JE 94k btc wallet.48FA4D | |
| 0048FA48 | 83E8 04 | SUB EAX,4 | eax: &"127.0.0.1:1604" |
| 0048FA4B | 8B00 | MOV EAX,DWORD PTR DS:[EAX] | eax: &"127.0.0.1:1604", [eax]: "127.0.0.1:1604" |
| 0048FA4D | 85C0 | TEST EAX,EAX | eax: &"127.0.0.1:1604" |
| 0048FA4F | 7E 10 | JLE 94k btc wallet.48FA61 | |
| 0048FA51 | A1 144C4900 | MOV EAX,DWORD PTR DS:[494C14] | eax: &"127.0.0.1:1604" |
| 0048FA56 | 8B15 E4C34900 | MOV EDX,DWORD PTR DS:[49C3E4] | 0049C3E4: &"kvejo991.ddns.net:1604" |
| 0048FA5C | E8 238F7FFF | CALL 94k btc wallet.405584 | |
| 0048FA61 | 8D55 B0 | LEA EDX,DWORD PTR SS:[EBP-50] | |
| 0048FA64 | B8 80064900 | MOV EAX,94k btc wallet.490680 | eax: &"127.0.0.1:1604", 490680: "SID" |
| 0048FA69 | E8 7A38FEFF | CALL 94k btc wallet.4735E8 | |
| 0048FA6E | 8B55 B0 | MOV EDX,DWORD PTR SS:[EBP-50] | |
| 0048FA71 | B8 E4C34900 | MOV EAX,94k btc wallet.49C3E4 | eax: &"127.0.0.1:1604", 49C3E4: &"kvejo991.ddns.net:1604" |
| 0048FA76 | E8 0958F7FF | CALL 94k btc wallet.405584 | |
| 0048FA7B | A1 E4C34900 | MOV EAX,DWORD PTR DS:[49C3E4] | eax: &"127.0.0.1:1604", 0049C3E4: &"kvejo991.ddns.net:1604" |
| 0048FA80 | 85C0 | TEST EAX,EAX | eax: &"127.0.0.1:1604" |
| 0048FA82 | 74 05 | JE 94k btc wallet.48FA89 | |
| 0048FA84 | 83E8 04 | SUB EAX,4 | eax: &"127.0.0.1:1604" |
| 0048FA87 | 8B00 | MOV EAX,DWORD PTR DS:[EAX] | eax: &"127.0.0.1:1604", [eax]: "127.0.0.1:1604" |
| 0048FA89 | 85C0 | TEST EAX,EAX | eax: &"127.0.0.1:1604" |
| 0048FA8B | 7E 12 | JLE 94k btc wallet.48FA9F | |
| 0048FA8D | A1 30494900 | MOV EAX,DWORD PTR DS:[494930] | eax: &"127.0.0.1:1604" |
| 0048FA92 | 8B15 E4C34900 | MOV EDX,DWORD PTR DS:[49C3E4] | 0049C3E4: &"kvejo991.ddns.net:1604" |
| 0048FA98 | E8 5F58F7FF | CALL 94k btc wallet.405584 | |

Figure 7: kvejo991.ddns.net:1604

| | | | |
|----------|---------------|-------------------------------|---|
| 0048FA6E | 8B55 B0 | mov edx,dword ptr ss:[ebp-50] | [ebp-50]: "AP" |
| 0048FA71 | B8 E4C34900 | mov eax,94k btc wallet.49C3E4 | eax:&"DC_Mutex-ARULYYD", 49C3E4:&"DC_Mutex-ARULYYD" |
| 0048FA76 | E8 095BF7FF | call 94k btc wallet.405584 | eax:&"DC_Mutex-ARULYYD", 0049C3E4:&"DC_Mutex-ARULYYD" |
| 0048FA7B | A1 E4C34900 | mov eax,dword ptr ds:[49C3E4] | eax:&"DC_Mutex-ARULYYD" |
| 0048FA80 | 85C0 | test eax,edx | |
| 0048FA82 | 74 05 | je 94k btc wallet.48FA89 | |
| 0048FA84 | 83E8 04 | sub eax,4 | eax:&"DC_Mutex-ARULYYD" |
| 0048FA87 | 8B00 | mov eax,dword ptr ds:[eax] | eax:&"DC_Mutex-ARULYYD", [eax]: "DC_Mutex-ARULYYD" |
| 0048FA89 | 85C0 | test eax,edx | eax:&"DC_Mutex-ARULYYD" |
| 0048FA8B | 7E 12 | jle 94k btc wallet.48FA9F | |
| 0048FA8D | A1 30494900 | mov eax,dword ptr ds:[494930] | eax:&"DC_Mutex-ARULYYD" |
| 0048FA92 | 8B15 E4C34900 | mov edx,dword ptr ds:[49C3E4] | edx: "AP", 0049C3E4:&"DC_Mutex-ARULYYD" |
| 0048FA98 | E8 E75AF7FF | call 94k btc wallet.405584 | |
| 0048FA9D | E8 0F | jmp 94k btc wallet.48FAAE | |
| 0048FA9F | A1 30494900 | mov eax,dword ptr ds:[494930] | eax:&"DC_Mutex-ARULYYD" |
| 0048FAA4 | BA BC064900 | mov edx,94k btc wallet.4906BC | edx: "AP", 4906BC: "Guest" |
| 0048FAA9 | E8 D65AF7FF | call 94k btc wallet.405584 | |
| 0048FAAE | 8D55 AC | lea edx,dword ptr ss:[ebp-54] | [ebp-54]: "DC_Mutex-ARULYYD" |
| 0048FAB1 | B8 CC064900 | mov eax,94k btc wallet.4906CC | eax:&"DC_Mutex-ARULYYD", 4906CC: "MUTEX" |
| 0048FAB6 | E8 2D3BF7FF | call 94k btc wallet.4735E8 | |
| 0048FAB8 | 8B55 AC | mov edx,dword ptr ss:[ebp-54] | [ebp-54]: "DC_Mutex-ARULYYD" |
| 0048FABE | B8 E4C34900 | mov eax,94k btc wallet.49C3E4 | eax:&"DC_Mutex-ARULYYD", 49C3E4:&"DC_Mutex-ARULYYD" |
| 0048FAC3 | E8 BC5AF7FF | call 94k btc wallet.405584 | |
| 0048FAC8 | A1 E4C34900 | mov eax,dword ptr ds:[49C3E4] | eax:&"DC_Mutex-ARULYYD", 0049C3E4:&"DC_Mutex-ARULYYD" |
| 0048FACD | 85C0 | test eax,edx | eax:&"DC_Mutex-ARULYYD" |
| 0048FACF | 74 05 | je 94k btc wallet.48FAD6 | |
| 0048FAD1 | 83E8 04 | sub eax,4 | eax:&"DC_Mutex-ARULYYD" |
| 0048FAD4 | 8B00 | mov eax,dword ptr ds:[eax] | eax:&"DC_Mutex-ARULYYD", [eax]: "DC_Mutex-ARULYYD" |
| 0048FAD6 | 85C0 | test eax,edx | eax:&"DC_Mutex-ARULYYD" |
| 0048FAD8 | 7E 12 | jle 94k btc wallet.48FAEC | |
| 0048FADA | A1 384D4900 | mov eax,dword ptr ds:[494D38] | eax:&"DC_Mutex-ARULYYD" |
| 0048FADF | 8B15 E4C34900 | mov edx,dword ptr ds:[49C3E4] | edx: "AP", 0049C3E4:&"DC_Mutex-ARULYYD" |
| 0048FAE5 | E8 9A5AF7FF | call 94k btc wallet.405584 | |
| 0048FAEA | E8 0F | jmp 94k btc wallet.48FAFB | |
| 0048FAEC | A1 384D4900 | mov eax,dword ptr ds:[494D38] | eax:&"DC_Mutex-ARULYYD" |
| 0048FAF1 | BA DC064900 | mov edx,94k btc wallet.4906DC | edx: "AP", 4906DC: "DCMUTEX" |
| 0048FAF6 | E8 895AF7FF | call 94k btc wallet.405584 | |
| 0048FAFB | 8D55 A4 | lea edx,dword ptr ss:[ebp-5C] | |
| 0048FAFE | B8 EC064900 | mov eax,94k btc wallet.4906EC | eax:&"DC_Mutex-ARULYYD", 4906EC: "EDTPATH" |

Figure 8: DC_Mutex-ARULYYD

| | | | |
|----------|---------------|-------------------------------|---|
| 0048FA9F | A1 30494900 | mov eax,dword ptr ds:[494930] | eax: "MSDCSC\\explorer.exe" |
| 0048FAA4 | BA BC064900 | mov edx,94k btc wallet.4906BC | edx: "EDTPATH", 4906BC: "Guest" |
| 0048FAA9 | E8 D65AF7FF | call 94k btc wallet.405584 | |
| 0048FAAE | 8D55 AC | lea edx,dword ptr ss:[ebp-54] | [ebp-54]: "DC_Mutex-ARULYYD" |
| 0048FAB1 | B8 CC064900 | mov eax,94k btc wallet.4906CC | eax: "MSDCSC\\explorer.exe", 4906CC: "MUTEX" |
| 0048FAB6 | E8 2D3BF7FF | call 94k btc wallet.4735E8 | |
| 0048FAB8 | 8B55 AC | mov edx,dword ptr ss:[ebp-54] | [ebp-54]: "DC_Mutex-ARULYYD" |
| 0048FABE | B8 E4C34900 | mov eax,94k btc wallet.49C3E4 | eax: "MSDCSC\\explorer.exe", 49C3E4:&"DC_Mutex-ARULYYD" |
| 0048FAC3 | E8 BC5AF7FF | call 94k btc wallet.405584 | |
| 0048FAC8 | A1 E4C34900 | mov eax,dword ptr ds:[49C3E4] | eax: "MSDCSC\\explorer.exe", 0049C3E4:&"DC_Mutex-ARULYYD" |
| 0048FACD | 85C0 | test eax,edx | eax: "MSDCSC\\explorer.exe" |
| 0048FACF | 74 05 | je 94k btc wallet.48FAD6 | |
| 0048FAD1 | 83E8 04 | sub eax,4 | eax: "MSDCSC\\explorer.exe" |
| 0048FAD4 | 8B00 | mov eax,dword ptr ds:[eax] | eax: "MSDCSC\\explorer.exe" |
| 0048FAD6 | 85C0 | test eax,edx | eax: "MSDCSC\\explorer.exe" |
| 0048FAD8 | 7E 12 | jle 94k btc wallet.48FAEC | |
| 0048FADA | A1 384D4900 | mov eax,dword ptr ds:[494D38] | eax: "MSDCSC\\explorer.exe" |
| 0048FADF | 8B15 E4C34900 | mov edx,dword ptr ds:[49C3E4] | edx: "EDTPATH", 0049C3E4:&"DC_Mutex-ARULYYD" |
| 0048FAE5 | E8 9A5AF7FF | call 94k btc wallet.405584 | |
| 0048FAEA | E8 0F | jmp 94k btc wallet.48FAFB | |
| 0048FAEC | A1 384D4900 | mov eax,dword ptr ds:[494D38] | eax: "MSDCSC\\explorer.exe" |
| 0048FAF1 | BA DC064900 | mov edx,94k btc wallet.4906DC | edx: "EDTPATH", 4906DC: "DCMUTEX" |
| 0048FAF6 | E8 895AF7FF | call 94k btc wallet.405584 | |
| 0048FAFB | 8D55 A4 | lea edx,dword ptr ss:[ebp-5C] | [ebp-5C]: "MSDCSC\\explorer.exe" |
| 0048FAFE | B8 EC064900 | mov eax,94k btc wallet.4906EC | eax: "MSDCSC\\explorer.exe", 4906EC: "EDTPATH" |
| 0048FB03 | E8 E03AF7FF | call 94k btc wallet.4735E8 | |
| 0048FB08 | 8B45 A4 | mov eax,dword ptr ss:[ebp-5C] | [ebp-5C]: "MSDCSC\\explorer.exe" |
| 0048FB0B | 50 | push eax | eax: "MSDCSC\\explorer.exe" |
| 0048FB0C | 8D55 A0 | lea edx,dword ptr ss:[ebp-60] | |
| 0048FB0F | B8 FC064900 | mov eax,94k btc wallet.4906FC | eax: "MSDCSC\\explorer.exe", 4906FC: "COMBOPATH" |
| 0048FB14 | E8 CF3AF7FF | call 94k btc wallet.4735E8 | |
| 0048FB19 | 8B45 A0 | mov eax,dword ptr ss:[ebp-60] | |
| 0048FB1C | 8D4D A8 | lea ecx,dword ptr ss:[ebp-58] | |
| 0048FB1F | 5A | pop ecx | edx: "EDTPATH" |
| 0048FB20 | E8 E759F7FF | call 94k btc wallet.48550C | |
| 0048FB25 | 8B55 A8 | mov edx,dword ptr ss:[ebp-58] | |
| 0048FB28 | A1 7C484900 | mov eax,dword ptr ds:[49487C] | eax: "MSDCSC\\explorer.exe" |
| 0048FB2D | E8 525AF7FF | call 94k btc wallet.405584 | |
| 0048FB32 | 8D55 9C | lea edx,dword ptr ss:[ebp-64] | |
| 0048FB35 | B8 80064900 | mov eax,94k btc wallet.490680 | eax: "MSDCSC\\explorer.exe", 490680: "GENCODE" |

Figure 9: MSDSC\\explorer.exe

Keylogging Activity Captured Logs

During analysis, it was observed that the malware component performs keylogging activity, where it records the victim's keystrokes to capture sensitive information such as login credentials, chat messages, or banking details.

The captured keystrokes are then stored locally inside a folder named **dclogs**, which acts as the malware's data repository before the logs are either exfiltrated to the command-and-control (C2) server or retained for local collection by the attacker.

Figure 10: Keystroke activities captured in log file

```

1  :: 94k BTC wallet.exe - PID: 2A24 - Module: windows.storage.dll - Thread: Main Thread 2E30 - x32dbg (02:47:47)
2  [F8]
3
4  :: 94k BTC wallet.exe - PID: 2A24 - Module: shell32.dll - Thread: Main Thread 2E30 - x32dbg (02:49:07)
5  [F8][F8][F8]
6
7  :: Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-IFHT1FF\VM] (02:49:41)
8
9
10 :: Windows (02:49:59)
11 syswow[LEFT][LEFT][LEFT][LEFT][LEFT][LEFT][LEFT][LEFT][LEFT][LEFT][LEFT][LEFT][LEFT]s[RIGHT][RIGHT][RIGHT][RIGHT][RIGHT]
12 [RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT]
13
14 :: SysWOW64 (02:50:23)
15 notepad
16
17 :: notepad - Search Results in SysWOW64 (02:52:59)
18 [REDACTED]
19
20 :: Clipboard Change : size = 14 Bytes (02:52:59)
21 94k BTC wallet
22
23 :: x32dbg (02:53:02)
24 r
25
26 :: Run (02:55:00)
27 %temp%
28
29
30 :: Roaming (03:00:29)
31
32
33 :: Task View (03:00:31)

```

Figure 11: Keystroke logs

Process Behavior of “94k BTC wallet.exe”

| | | | | | |
|--------------------|------|----------|----------|------------------------------------|--------------------------------|
| procexp64.exe | 0.76 | 24,680 K | 50,216 K | 5676 Sysinternals Process Explorer | Sysinternals - www.sysinter... |
| 94k BTC wallet.exe | 2.52 | 6,280 K | 22,588 K | 9328 Remote Service Application | Microsoft Corp. |
| cmd.exe | 0.25 | 4,784 K | 5,352 K | 6376 Windows Command Process... | Microsoft Corporation |
| conhost.exe | 1.01 | 6,748 K | 15,440 K | 8720 Console Window Host | Microsoft Corporation |
| cmd.exe | 0.25 | 4,788 K | 5,352 K | 6892 Windows Command Process... | Microsoft Corporation |
| conhost.exe | 0.76 | 6,740 K | 15,424 K | 8924 Console Window Host | Microsoft Corporation |
| notepad.exe | 0.25 | 3,812 K | 12,212 K | 6908 Notepad | Microsoft Corporation |

Figure 12: DarkComet initiates a stealthy injection chain, spawning multiple processes to cloak its malicious payload behind a deceptive interface.

Upon execution, the “94k BTC wallet.exe” spawns multiple cmd.exe and conhost.exe processes, as seen in the process hierarchy. These child processes indicate that the malware executes a series of internal commands to establish its runtime environment.

After the command shells are spawned, the malware further launches notepad.exe, which is a known decoy process behavior of DarkComet. The RAT injects its payload into Notepad’s process space to perform actions such as keylogging, screen capture, and remote command execution, while keeping activity hidden under a legitimate Windows process.

Command-and-Control (C2) Communication

During network analysis, the unpacked DarkComet sample was observed attempting to establish a TCP connection to kvejo991.ddns.net on port 1604, which aligns with the default command-and-control (C2) port commonly used by the DarkComet RAT family. The connection logs showed multiple retransmissions, suggesting that the remote server was either offline or blocking incoming connections at the time of execution. Despite the failed connection, these repeated attempts clearly indicate active C2 beaconing behavior, confirming that the malware was trying to communicate with its operator to receive commands or exfiltrate data—behavior that is consistent with known DarkComet RAT activity patterns.

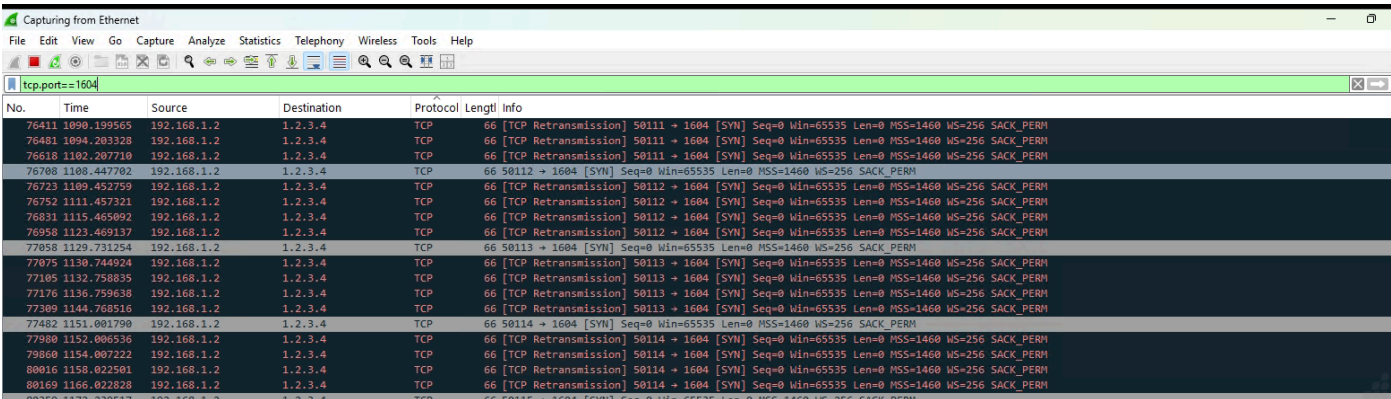


Figure 13: Network traffic on Port 1604

Indicators of Compromise (IOCs)

| Category | Indicator |
|----------------------------|---|
| Archive File | 11bf1088d66bc3a63d16cc9334a05f214a25a47f39713400279e0823c97eb377 |
| Payload EXE | 5b5c276ea74e1086e4835221da50865f872fe20cfc5ea9aa6a909a0b0b9a0554 |
| Unpacked EXE | 58c284e7bbeacb5e1f91596660d33d0407d138ae0be545f59027f8787da75eda |
| Install Path | C:\Users\<User>\AppData\Roaming\MSDCSC\explorer.exe |
| Registry Key | HKCU\Software\Microsoft\Windows\CurrentVersion\Run\explorer -> C:\Users\admin\AppData\Roaming\MSDCSC\explorer.exe |
| Mutex | DC_MUTEX-ARULYYD |
| C2 Domain | kvejo991.ddns.net |
| C2 Port | 1604 (TCP) |
| Keystroke Capture Log file | 2025-10-29-4.dc |

MITRE ATT&CK Mapping

| Tactic | Techniques | ID | Relevance in Sample |
|---------------------|---|-----------|--|
| Initial Access | Spearphishing Attachment (Compressed Archive) | T1566.001 | Delivered as a malicious RAR file attachment/download to lure victims with the Bitcoin tool theme. |
| Defense Evasion | Obfuscated/Compressed Binary – UPX Packing | T1027.002 | The payload was packed with UPX to evade static detection. |
| Execution | User Execution | T1204 | The victim manually extracts and runs the disguised Bitcoin application. |
| Persistence | Registry Run Keys / Startup Folder | T1547.001 | DarkComet sets autostart entries to survive reboots. |
| Collection | Keylogging | T1056.001 | Primary behavior observed: keystroke capture for credential and wallet theft |
| Command and Control | Application Layer Protocol | T1071.001 | Establishes connection with C2 domain over TCP. |
| Command and Control | Exfiltration Over C2 Channel | T1041 | Captured keystrokes and data are exfiltrated via the same C2 connection. |

Removal

1. Reboot into Safe Mode with Networking.
2. Use updated UltraAV.
3. UltraAV unpacked a UPX-packed executable into the TempData folder and detected the malicious payload with following name:

Backdoor.DarkComet

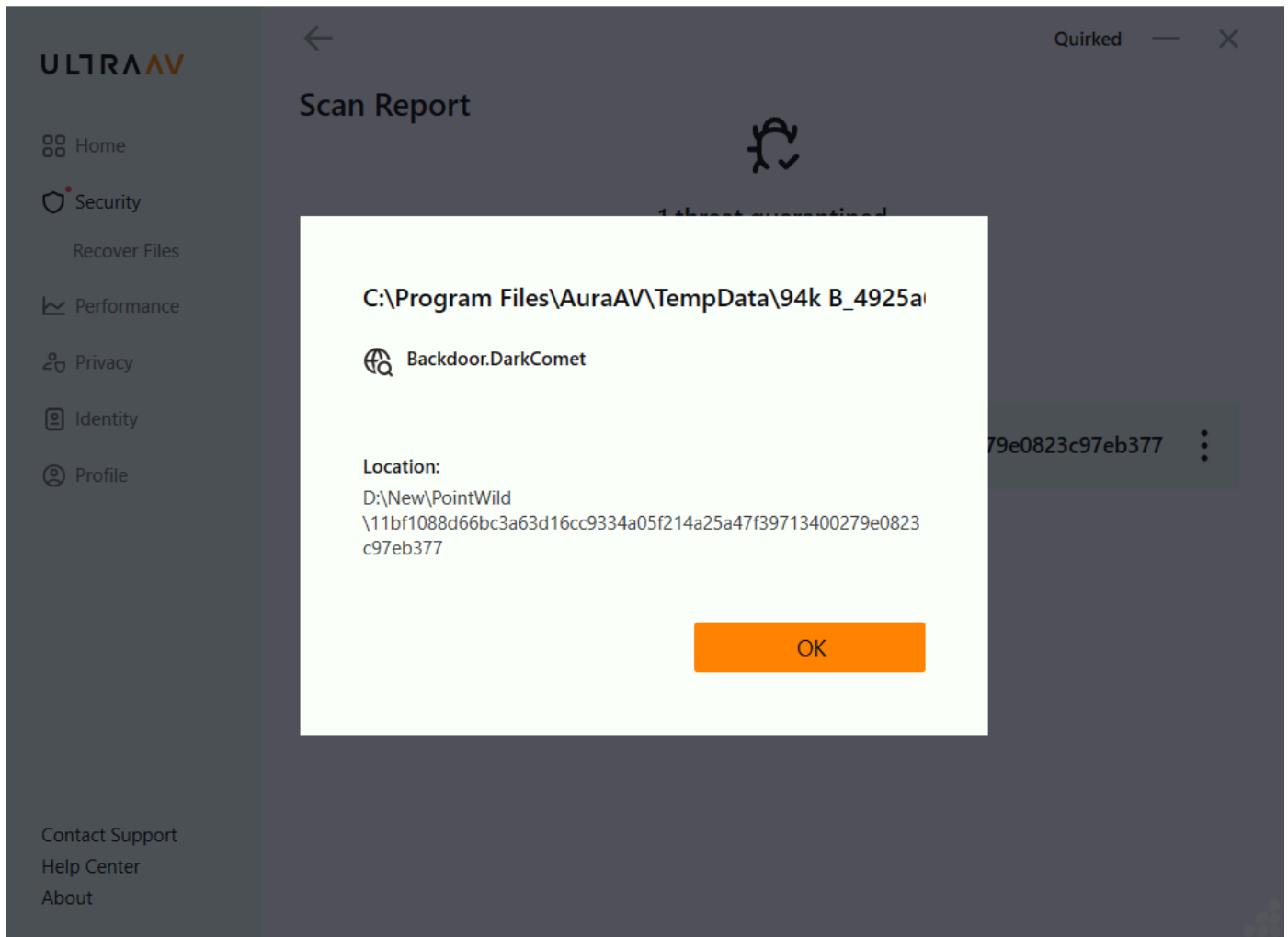


Figure 14: Ultra AV Detection

Conclusion

The analysis of this Bitcoin themed DarkComet RAT sample demonstrates how old malware families continue to find new life through modern lures. By hiding inside a file packaged as a cryptocurrency utility, the attacker leveraged the ongoing hype around Bitcoin to trick users into executing a well established remote access trojan. Although DarkComet is not a new threat, its feature set remains dangerous: keylogging, credential theft, file manipulation, surveillance, and persistence techniques are still effective against unsuspecting victims. Combined with the lure of cryptocurrency applications, this makes the malware especially impactful, since compromised systems may lead directly to stolen wallet credentials and financial losses.